Polityka cyberbezpieczeństwa

Cyberbezpieczeństwo stanowi integralny element misji Elektrociepłowni Ciechanów Sp. z o.o., której nadrzędnym celem jest zapewnienie ciągłości, niezawodności i bezpieczeństwa dostaw energii cieplnej oraz energii elektrycznej dla mieszkańców miasta i jednostek gminnych. W dobie rosnących zagrożeń cyfrowych Spółka traktuje ochronę informacji, systemów IT/OT oraz infrastruktury krytycznej jako fundament stabilności operacyjnej i odpowiedzialności wobec społeczności lokalnej.

Priorytety Spółki w obszarze cyberbezpieczeństwa to:

- zapewnienie odporności systemów IT/OT na incydenty i zagrożenia,
- ochrona infrastruktury krytycznej i procesów technologicznych,
- utrzymanie ciągłości działania i bezpieczeństwa dostaw,
- budowanie kultury bezpieczeństwa wśród pracowników, kontrahentów i partnerów,
- spełnienie wymagań wynikających z ustawy o KSC, dyrektywy NIS2 oraz norm ISO 27001/27019.

Spółka realizuje tę misję poprzez rozwój kompetencji, wdrażanie nowoczesnych rozwiązań technicznych, systematyczne doskonalenie procesów oraz współpracę z wyspecjalizowanymi podmiotami w zakresie monitorowania i reagowania na incydenty.

Cele w obszarze cyberbezpieczeństwa

W ramach realizacji misji Spółka dąży do:

- zapewnienia wysokiego poziomu ochrony systemów sterowania, automatyki i infrastruktury OT,
- wdrożenia i utrzymania systemu zarządzania bezpieczeństwem informacji zgodnego z ISO 27001/27019,
- skutecznego zarządzania ryzykiem cybernetycznym,
- monitorowania zagrożeń i incydentów we współpracy z SOC,
- zapewnienia bezpiecznej współpracy z dostawcami i wykonawcami,
- ochrony danych osobowych i informacji wrażliwych,
- ciągłego podnoszenia świadomości pracowników i kontrahentów.

Odpowiedzialność społeczna w obszarze cyberbezpieczeństwa

Elektrociepłownia Ciechanów Sp. z o.o. postrzega cyberbezpieczeństwo jako element odpowiedzialności wobec mieszkańców, odbiorców usług oraz partnerów biznesowych. Ochrona infrastruktury krytycznej i danych jest nie tylko obowiązkiem prawnym, ale również wyrazem troski o bezpieczeństwo społeczności lokalnej.

Spółka:

- prowadzi działania edukacyjne w zakresie cyberhigieny dla pracowników i wykonawców,
- wspiera inicjatywy lokalne związane z bezpieczeństwem cyfrowym i technologicznym,

- współpracuje z instytucjami publicznymi i służbami odpowiedzialnymi za bezpieczeństwo,
- promuje odpowiedzialne korzystanie z technologii i ochronę danych,

Priorytetowe wartości w obszarze cyberbezpieczeństwa

1. **Odpowiedzialność za bezpieczeństwo infrastruktury krytycznej.**
2. **Ochrona informacji i danych osobowych.**
3. **Bezpieczeństwo pracowników, odbiorców i partnerów.**
4. **Transparentność działań i zgodność z przepisami prawa.**
5. **Ciągłe doskonalenie kompetencji i procesów.**

W ramach tych wartości Spółka kieruje się zasadami:

- rzetelności i staranności w ochronie systemów,
- poufności, integralności i dostępności informacji,
- terminowego reagowania na incydenty,
- współpracy i wymiany informacji z podmiotami odpowiedzialnymi za bezpieczeństwo,
- uczciwości i przejrzystości w relacjach z kontrahentami,
- dążenia do rozwoju technologicznego i organizacyjnego.